Les bases de la cryptographie

Ce sujet est le fruit d'un travail inédit, en cours d'élaboration, qui devra probablement être affiné.

Le but de la cryptographie est de brouiller un message pour en garantir sa confidentialité, son authenticité et son intégrité. Cela passe donc forcément par des processus techniques mais aussi et surtout, par un comportement adéquat qui garantira l'objectif de sécurité que l'on recherche à atteindre.

Pour prendre les choses dans l'ordre, il est nécessaire de commencer par le comportement. Dans le comportement, nous incluons les mesures organisationnelles qui accompagnent la sécurité de la cryptographie. Le comportement induit les mesures organisationnelles adéquates.

La sécurité (généralité)

Avant d'aller plus avant, il est nécessaire de définir la sécurité elle-même.

La sécurité est un concept qui vise à supprimer tout risque et tout danger à l'encontre de ce qu'elle est sensé protéger à un moment donné. Elle est généralement mise en œuvre par :

- une conception spécifique de l'objet à protéger pour minimiser les risques ;
- un ou plusieurs systèmes externes ayant pour but la protection de l'objet à protéger ;
- une conception spécifique des objets voisins pour minimiser les risques sur l'objet à protéger ;
- un cadre comportemental visant à minimiser les risques sur l'objet à protéger.

On comprend alors que l'on ne peut que réduire les risques, mais jamais les éliminer complètement. Même s'il est potentiellement possible de réduire les risques à un niveau extrêmement bas à un moment donné, l'objet protégé sera exposé dans un futur plus ou moins proche. La sécurité d'un objet, qui n'est jamais absolue, se dégrade avec le temps.

Parmi les plus grands dangers qui menace la sécurité il y a : * la suffisance d'expert qui pense que, à eux-seuls, ils sont capables d'anticiper toutes menace et sans jamais faire d'erreur ;

- la certitude que la sécurité peut-être absolue ;
- l'illusion de la sécurité.

Diverses approches sécuritaires

Quand on parle de sécurité, il faut commencer par choisir une approche et évaluer sa pertinence. Il n'y a que 2 approches possibles :

- la sécurité par l'obscurité ;
- la sécurité par l'ouverture et la transparence.

Le concept de “sécurité par l'obscurité” qui repose sur la non-divulgation d'information relative à la structure, au fonctionnement et à l'implémentation de l'objet ou du procédé considéré pour en

assurer sa sécurité. Comme nous l'a montré l'histoire et ce que l'on constate encore aujourd'hui, cette approche est très hasardeuse et peu fiable.

Le concept d'ouverture correspond au “principe de Kerckhoffs” (énoncé par Auguste Kerckhoffs). Ce principe exprime que la sécurité d'un cryptosystème ne doit reposer que sur le secret de la clef. Autrement dit, tous les autres paramètres doivent être supposés publiquement connus. Il a été reformulé, peut-être indépendamment, par Claude Shannon : “l'adversaire connaît le système”. Cette formulation est connue sous le nom de la “maxime de Shannon”. Il est considéré aujourd'hui comme un principe fondamental par les cryptologues et s'oppose à la sécurité par l'obscurité. La tendance actuelle considère que quand les systèmes de chiffrement sont publics, largement étudiés et qu'aucune attaque significative n'est connue, ils sont d'autant plus sûrs.

Le “principe de Kerckhoffs” est relatif à la cryptologie. Cependant, il est transposable à tout système de sécurité.

La qualité reconnue de nombreux logiciels libres en matière de sécurité, est une bonne illustration que l'ouverture ne nuit pas et qu'elle a comme effet de renforcer la sécurité. Nous préconisons de rejeter la “sécurité par l'obscurité”. Nous pouvons donc déjà exclure cette approche.

Règles comportementales

Au niveau comportemental, la toute première chose est de prendre en compte les différents aspects qui ont été énumérés précédemment. Il faut donc faire des choix allant dans le sens de la sécurité. Avec l'informatique en générale, tout programme installé et exécuté sur son propre ordinateur est une menace potentielle à la sécurité de son propre système et des éléments qui le composent. Le matériel informatique et les programmes sont tous des objets voisins pouvant directement ou indirectement se mettre réciproquement en danger.

Ainsi, selon le “principe de Kerckhoffs” l'ordinateur ne peut qu'inclure des programmes et des logiciels ouverts. Ainsi, ce dernier ne peut être composé que de logiciels libres. Il est peut-être bon de rappeler que les logiciels propriétaires (privateurs) relèvent tous du concept de “sécurité par l'obscurité”, mais qu'en plus, nous savons qu'une grande majorité d'entre eux sont des logiciels malveillants. Il est aussi nécessaire de se prémunir des menaces venant du web en bloquant l'exécution des programmes Adobe Flash, Java et JavaScript qui sont intrinsèquement des failles de sécurités. Il est encore nécessaire de ne permettre que des courriels en texte brut (*plain text* en anglais) et d'exclure les courriels HTML. Ces quelques éléments particulièrement simples, qui ne relèvent que du choix de chacun, permettent une bonne protection de votre système informatique. Nous consacrerons, le plus rapidement possible, une page spécifique à ce sujet.

Bientôt la suite...